UNITED STATES DEPARTMENT OF AGRICULTURE
Farm Service Agency
Washington, DC 20250

Notice IRM-374

For: All FSA COC and STC Members and Advisers

Mandatory Privacy Act Training for COC and STC Members and Advisers

Approved by: Acting Administrator

Thomas B Hofeller

1 Overview

A Background

All FSA COC and STC members and advisers have a significant responsibility to ensure that:

- sensitive data entrusted to them is secure

- both FSA customers and employees sensitive personal data is not divulged to unauthorized personnel, lost, or stolen.

Notice IRM-371 provides FSA policy on the management of sensitive (Privacy Act protected) data to help safeguard the information. All FSA employees, contract employees, and partners who handle Privacy Act protected data in the performance of their duties **must** comply with this and all other applicable Federal, USDA, FSA, and OCIO ITS requirements.

The attached memorandum from the USDA Chief Information Officer requires that all USDA employees and contractors complete mandatory Privacy Act training. The AgLearn "USDA Privacy Basics" course is designated as mandatory training for FY 2006 and **must** be completed **no later than August 23, 2006**. This deadline is established to allow time for FSA to certify to the Department that 100 percent of our COC and STC members and advisers have completed training before **September 15, 2006**.

This notice applies **only** to COC and STC members and advisers. Training for Federal employees and contractors is addressed in a separate notice.

B Purpose

This notice:

- explains the mandatory FY 2006 Privacy Act training requirements
- provides procedures for COC and STC members and advisers to complete the training
- provides contact information
- explains how State AgLearn administrators will update AgLearn to document training.

Disposal Date	Distribution
October 1, 2007	All FSA COC and STC members and advisers; State Offices relay to County Offices

1 Overview (Continued)

C References

Procedure references are:

- The Privacy Act of 1974, as amended (Pub. L. 93-579, 5 U.S.C. 552a)
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, dated June 23, 2006
- Memorandum for all USDA employees and contractors from the CIO about "Protecting and Safeguarding Privacy Act Protected Information," dated July 18, 2006 (see Exhibit 1)
- Memorandum for all USDA employees and contractors from the CIO about "Protecting and Safeguarding Privacy Act Protected Information," dated June 16, 2006
- USDA Cyber Security Manual Series 3500
- Notice IRM-371
- Notice IRM-364
- Security Incident Response Guide for Users (see Exhibit 2).

D SED's Responsibilities

SED's must:

- certify in writing (by e-mail or memorandum) to DAFO, Attention: Ragh Singh that all **COC and STC members and advisers** have completed the mandatory Privacy Act training by **August 23, 2006**
- ensure that **new** COC and STC members and advisers complete the mandatory Privacy Act training within 30 workdays of their start date

  Note: This certification is expected to be required to support future audits of mandatory Privacy Act training requirements.

2 Training for STC, COC and any Others Without Access to AgLearn

A Training Materials

Soft copies of the Privacy Act training materials were e-mailed from DAFO to each State Office. State Offices will relay the training materials to the County Offices. Additionally, DAFO has posted the training materials to **http://intranet.fsa.usda.gov/fsatraining**.

B Deadline for Completing Training

All COC and STC members and advisers **must** complete the required Privacy Act training by **August 23, 2006**. If a member or advisor is out of the office the entire time between the date this notice is issued and **August 23, 2006**, then they should take the training immediately upon return to the office.

C Documenting COC and STC Member Privacy Act Training

After COC and STC members and advisors have reviewed the Privacy Act training materials, the State AgLearn administrator will use the Learning Event Recorder to update the learning history to show that the training has been completed. State AgLearn administrators shall log into AgLearn and follow theses steps to document COC and STC members and advisors training.

Step	Action
1	CLICK "Learning Management" from the top of the menu.
2	CLICK "Learning Event Recorder".
3	CLICK button Item, CLICK "Next", and CLICK on the picker next to Item Type.
4	Under Item ID, ENTER "USDA-Pri" and CLICK "Search".
5	CLICK "USDA-Privacy-Basics-Paper" and CLICK next.
6	In the Default Completion Status drop-down box CLICK "Course Pass for Credit".
7	Select the completion date, if needed to change, and CLICK "Next".
8	Under Add Learners and CLICK "Select from List".
9	ENTER employee's last name, CLICK "Search", CLICK next to the employee user is updating, and CLICK "Add". **Note:** Repeat this step until all names of employees user is updating are shown and CLICK "Next".
10	A list will be displayed, CLICK "Next".
11	The financial information will be displayed, CLICK "Next".
12	A summary of names will be displayed, CLICK "Finish". **Note:** The records have now been updated.

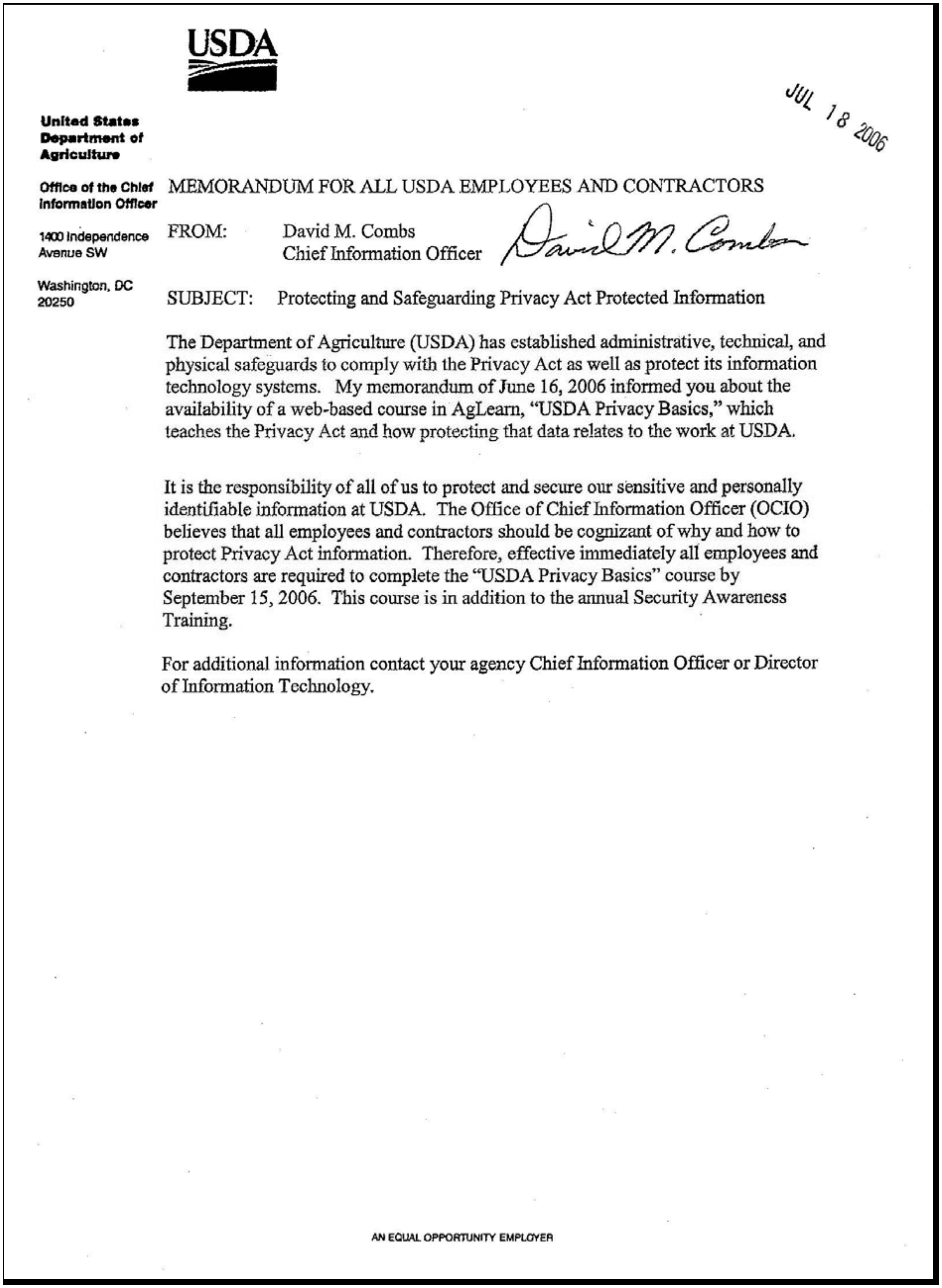
D Point of Contact and Additional Information

Direct Privacy Act policy questions to Norma Ferguson, FSA's FOIA/Privacy Act Officer, at 202-720-5534.

State and County Offices may contact Ruby Hervey, KCHRO, training coordinator, at **ruby.hervey@kcc.usda.gov** or 816-926-2834.

Exhibit 1

Memorandum About Protecting and Safeguarding Privacy Act Protected Information



USDA

JUL 18 2006

**United States
Department of
Agriculture**

**Office of the Chief
Information Officer**

1400 Independence
Avenue SW

Washington, DC
20250

MEMORANDUM FOR ALL USDA EMPLOYEES AND CONTRACTORS

FROM: David M. Combs
Chief Information Officer David M. Combs

SUBJECT: Protecting and Safeguarding Privacy Act Protected Information

The Department of Agriculture (USDA) has established administrative, technical, and physical safeguards to comply with the Privacy Act as well as protect its information technology systems. My memorandum of June 16, 2006 informed you about the availability of a web-based course in AgLearn, "USDA Privacy Basics," which teaches the Privacy Act and how protecting that data relates to the work at USDA.

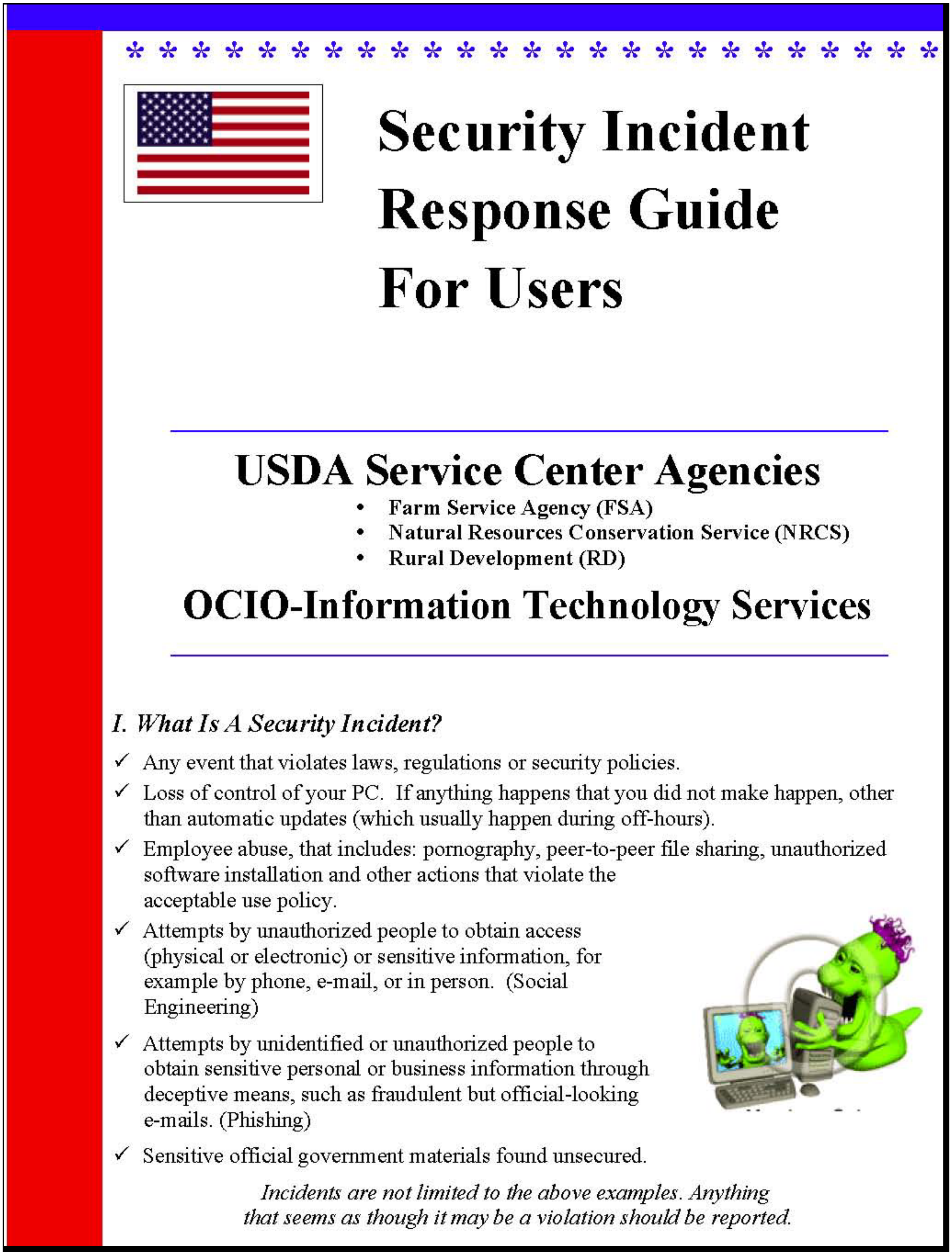
It is the responsibility of all of us to protect and secure our sensitive and personally identifiable information at USDA. The Office of Chief Information Officer (OCIO) believes that all employees and contractors should be cognizant of why and how to protect Privacy Act information. Therefore, effective immediately all employees and contractors are required to complete the "USDA Privacy Basics" course by September 15, 2006. This course is in addition to the annual Security Awareness Training.

For additional information contact your agency Chief Information Officer or Director of Information Technology.

AN EQUAL OPPORTUNITY EMPLOYER

Exhibit 2

Security Incident Response Guide for Users



Security Incident Response Guide For Users

USDA Service Center Agencies

- Farm Service Agency (FSA)
- Natural Resources Conservation Service (NRCS)
- Rural Development (RD)

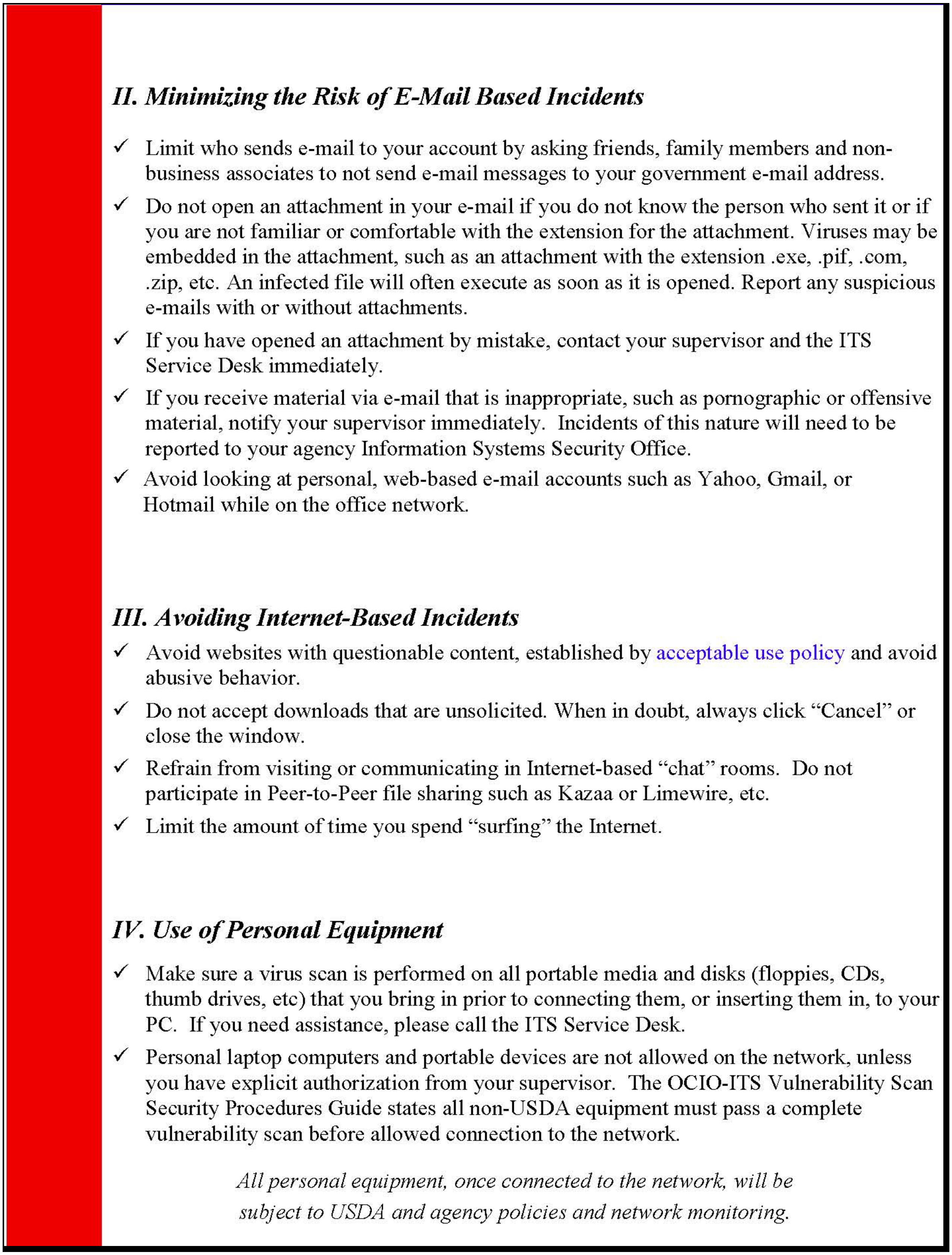
OCIO-Information Technology Services

I. What Is A Security Incident?

- ✓ Any event that violates laws, regulations or security policies.
- ✓ Loss of control of your PC. If anything happens that you did not make happen, other than automatic updates (which usually happen during off-hours).
- ✓ Employee abuse, that includes: pornography, peer-to-peer file sharing, unauthorized software installation and other actions that violate the acceptable use policy.
- ✓ Attempts by unauthorized people to obtain access (physical or electronic) or sensitive information, for example by phone, e-mail, or in person. (Social Engineering)
- ✓ Attempts by unidentified or unauthorized people to obtain sensitive personal or business information through deceptive means, such as fraudulent but official-looking e-mails. (Phishing)
- ✓ Sensitive official government materials found unsecured.

Incidents are not limited to the above examples. Anything that seems as though it may be a violation should be reported.

Security Incident Response Guide for Users (Continued)



II. Minimizing the Risk of E-Mail Based Incidents

- ✓ Limit who sends e-mail to your account by asking friends, family members and non-business associates to not send e-mail messages to your government e-mail address.
- ✓ Do not open an attachment in your e-mail if you do not know the person who sent it or if you are not familiar or comfortable with the extension for the attachment. Viruses may be embedded in the attachment, such as an attachment with the extension .exe, .pif, .com, .zip, etc. An infected file will often execute as soon as it is opened. Report any suspicious e-mails with or without attachments.
- ✓ If you have opened an attachment by mistake, contact your supervisor and the ITS Service Desk immediately.
- ✓ If you receive material via e-mail that is inappropriate, such as pornographic or offensive material, notify your supervisor immediately. Incidents of this nature will need to be reported to your agency Information Systems Security Office.
- ✓ Avoid looking at personal, web-based e-mail accounts such as Yahoo, Gmail, or Hotmail while on the office network.

III. Avoiding Internet-Based Incidents

- ✓ Avoid websites with questionable content, established by acceptable use policy and avoid abusive behavior.
- ✓ Do not accept downloads that are unsolicited. When in doubt, always click “Cancel” or close the window.
- ✓ Refrain from visiting or communicating in Internet-based “chat” rooms. Do not participate in Peer-to-Peer file sharing such as Kazaa or Limewire, etc.
- ✓ Limit the amount of time you spend “surfing” the Internet.

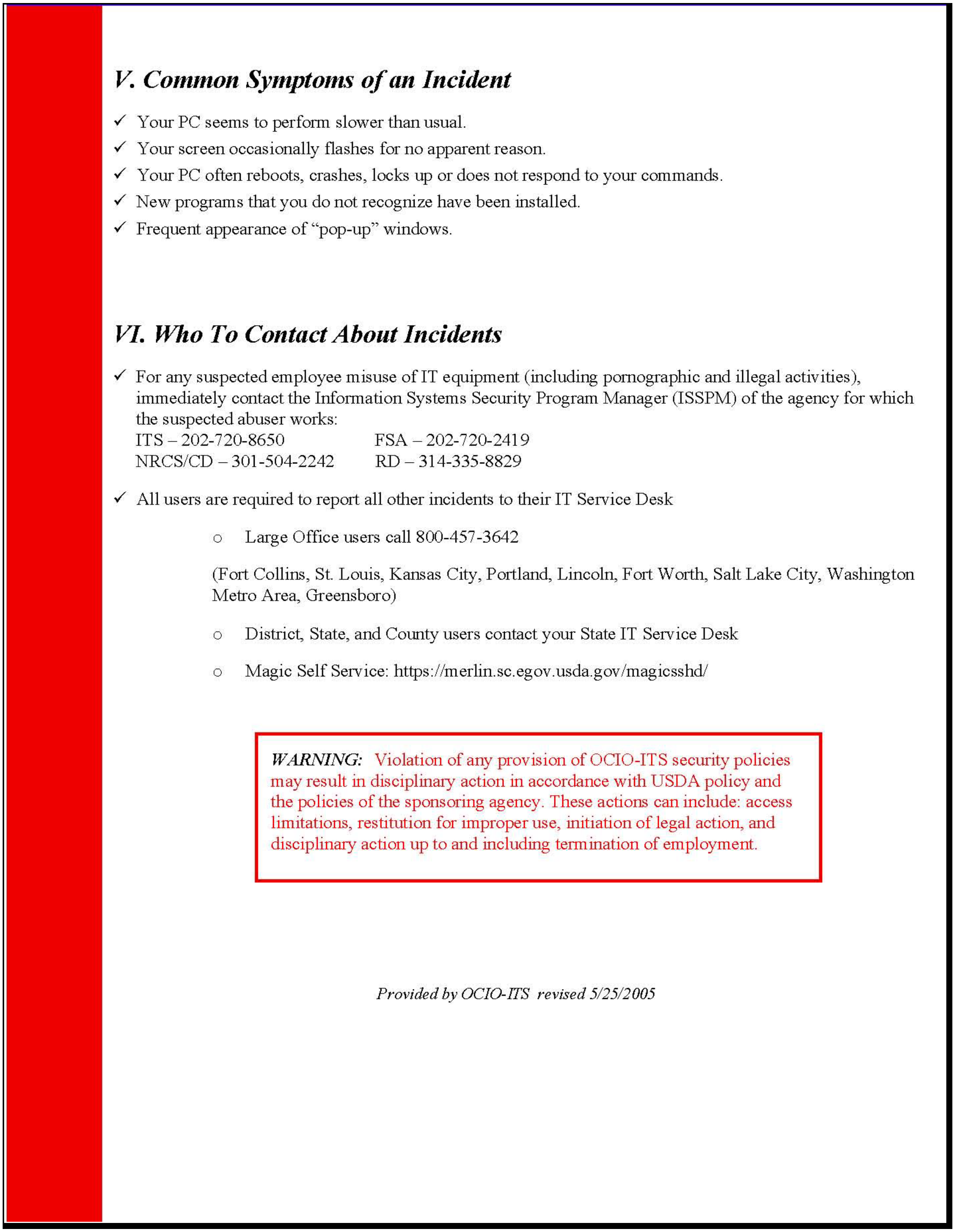
IV. Use of Personal Equipment

- ✓ Make sure a virus scan is performed on all portable media and disks (floppies, CDs, thumb drives, etc) that you bring in prior to connecting them, or inserting them in, to your PC. If you need assistance, please call the ITS Service Desk.
- ✓ Personal laptop computers and portable devices are not allowed on the network, unless you have explicit authorization from your supervisor. The OCIO-ITS Vulnerability Scan Security Procedures Guide states all non-USDA equipment must pass a complete vulnerability scan before allowed connection to the network.

All personal equipment, once connected to the network, will be subject to USDA and agency policies and network monitoring.

Exhibit 2

Security Incident Response Guide for Users (Continued)



V. Common Symptoms of an Incident

- ✓ Your PC seems to perform slower than usual.
- ✓ Your screen occasionally flashes for no apparent reason.
- ✓ Your PC often reboots, crashes, locks up or does not respond to your commands.
- ✓ New programs that you do not recognize have been installed.
- ✓ Frequent appearance of "pop-up" windows.

VI. Who To Contact About Incidents

- ✓ For any suspected employee misuse of IT equipment (including pornographic and illegal activities), immediately contact the Information Systems Security Program Manager (ISSPM) of the agency for which the suspected abuser works:

ITS – 202-720-8650	FSA – 202-720-2419
NRCS/CD – 301-504-2242	RD – 314-335-8829

- ✓ All users are required to report all other incidents to their IT Service Desk

  - ○ Large Office users call 800-457-3642

    (Fort Collins, St. Louis, Kansas City, Portland, Lincoln, Fort Worth, Salt Lake City, Washington Metro Area, Greensboro)

  - ○ District, State, and County users contact your State IT Service Desk

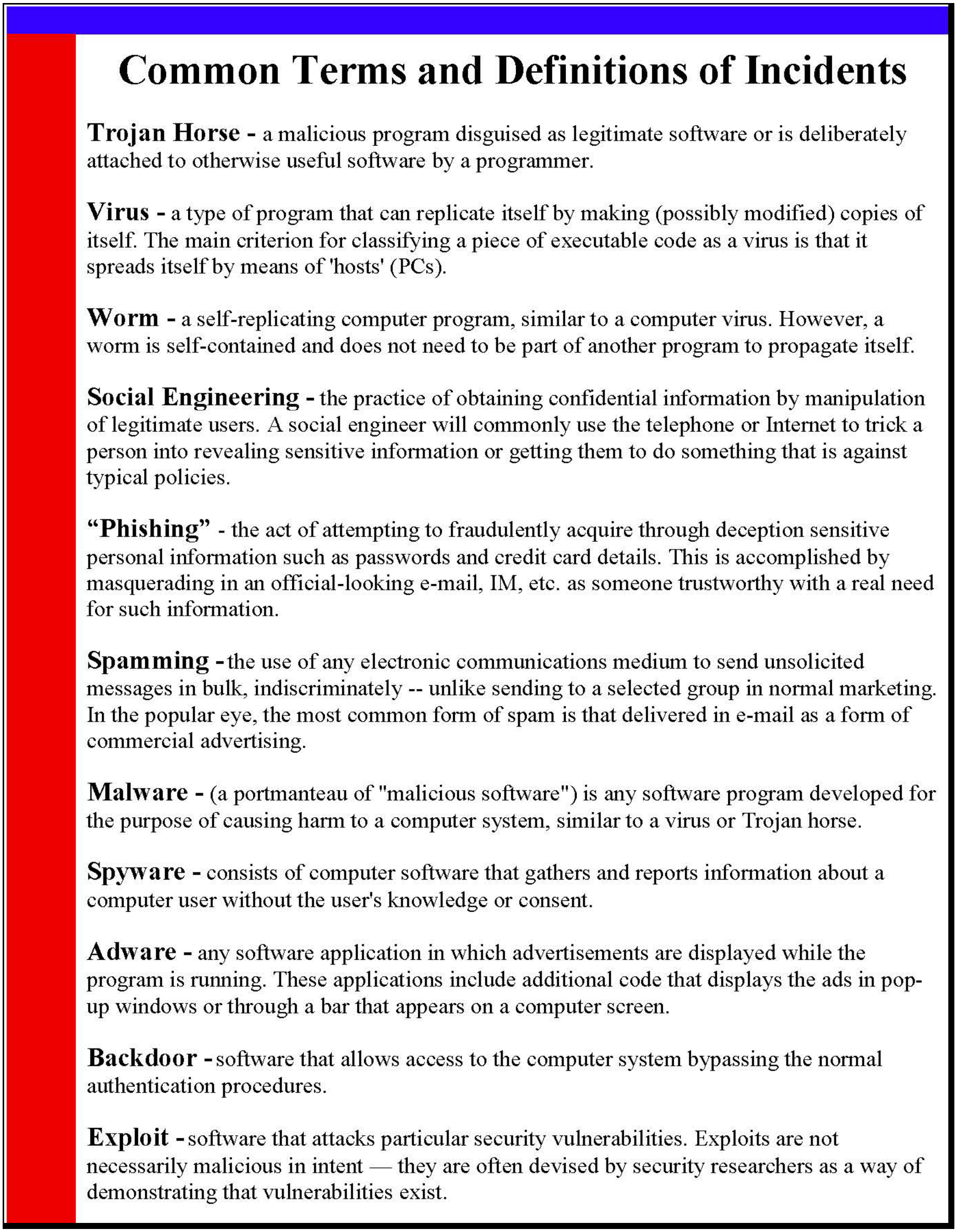
  - ○ Magic Self Service: https://merlin.sc.egov.usda.gov/magicsshd/

WARNING: Violation of any provision of OCIO-ITS security policies may result in disciplinary action in accordance with USDA policy and the policies of the sponsoring agency. These actions can include: access limitations, restitution for improper use, initiation of legal action, and disciplinary action up to and including termination of employment.

Provided by OCIO-ITS revised 5/25/2005

Exhibit 2

Security Incident Response Guide for Users (Continued)



Common Terms and Definitions of Incidents

Trojan Horse - a malicious program disguised as legitimate software or is deliberately attached to otherwise useful software by a programmer.

Virus - a type of program that can replicate itself by making (possibly modified) copies of itself. The main criterion for classifying a piece of executable code as a virus is that it spreads itself by means of 'hosts' (PCs).

Worm - a self-replicating computer program, similar to a computer virus. However, a worm is self-contained and does not need to be part of another program to propagate itself.

Social Engineering - the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies.

"Phishing" - the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details. This is accomplished by masquerading in an official-looking e-mail, IM, etc. as someone trustworthy with a real need for such information.

Spamming - the use of any electronic communications medium to send unsolicited messages in bulk, indiscriminately -- unlike sending to a selected group in normal marketing. In the popular eye, the most common form of spam is that delivered in e-mail as a form of commercial advertising.

Malware - (a portmanteau of "malicious software") is any software program developed for the purpose of causing harm to a computer system, similar to a virus or Trojan horse.

Spyware - consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent.

Adware - any software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen.

Backdoor - software that allows access to the computer system bypassing the normal authentication procedures.

Exploit - software that attacks particular security vulnerabilities. Exploits are not necessarily malicious in intent — they are often devised by security researchers as a way of demonstrating that vulnerabilities exist.